REMARKS

Claims 1-6 are pending in the above-identified patent application. Claims 1 has been amended and claim 3 has been canceled by way of the present amendment. Reconsideration is respectfully requested.

In the outstanding Office Action, claim 3 was objected to because the claim language is confusing; claims 1-4 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention; and claims 1-6 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,604,807 (Yamaguchi et al.).

Claim Objections

Claim 3 was objected to because the claim language is confusing. Claim 3 has been canceled by way of the present amendment. Therefore, it is respectfully requested that the outstanding rejection be withdrawn because the rejection is moot in lieu of the cancellation of claim 3.

35 U.S.C. § 112 Claim Rejections

Claims 1-4 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

Claim 3 has been canceled and incorporated into claim 1, which has been further amended to clarify the invention. In particular, claim 1 has been amended to recite:

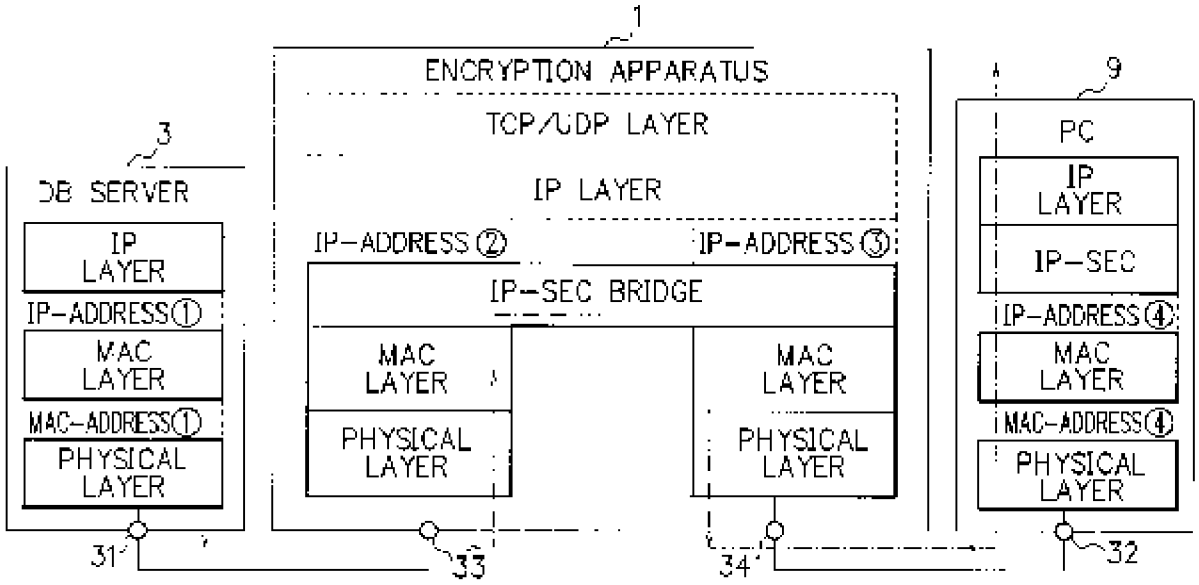
> the apparatus including encryption/decryption means for performing an encrypting process and a decrypting process on data to terminate encryption-based security between the communications terminals having the encrypting capability and/or

the non-encrypting capability~~encryption apparatus and the communications terminal having the encrypting capability~~; and . . . . wherein the encryption apparatus further includes bridge means for allowing data to be outputted as it is from another port without any routing process; and

wherein the data has been received with one of the plurality of ports of the encryption apparatus and the encrypting or decrypting process has been performed on the data.

Support for the amendment is provided in the original application and figures. That is, as shown in **FIG. 5**, the encryption apparatus **1** of this embodiment is characterized in that the IP-Sec serves as a bridge which links the two ports **33** and **34**, and wherein the term "bridge" indicates a function of sending data just as it is (which has inputted therein via one of the ports and then on which the encrypting or decrypting process has been performed) to another port without performing any routing process.[1]

F I G. 5



[1] *See* Specification at **FIG. 5** and paragraphs **[0009]** and **[0087]**.

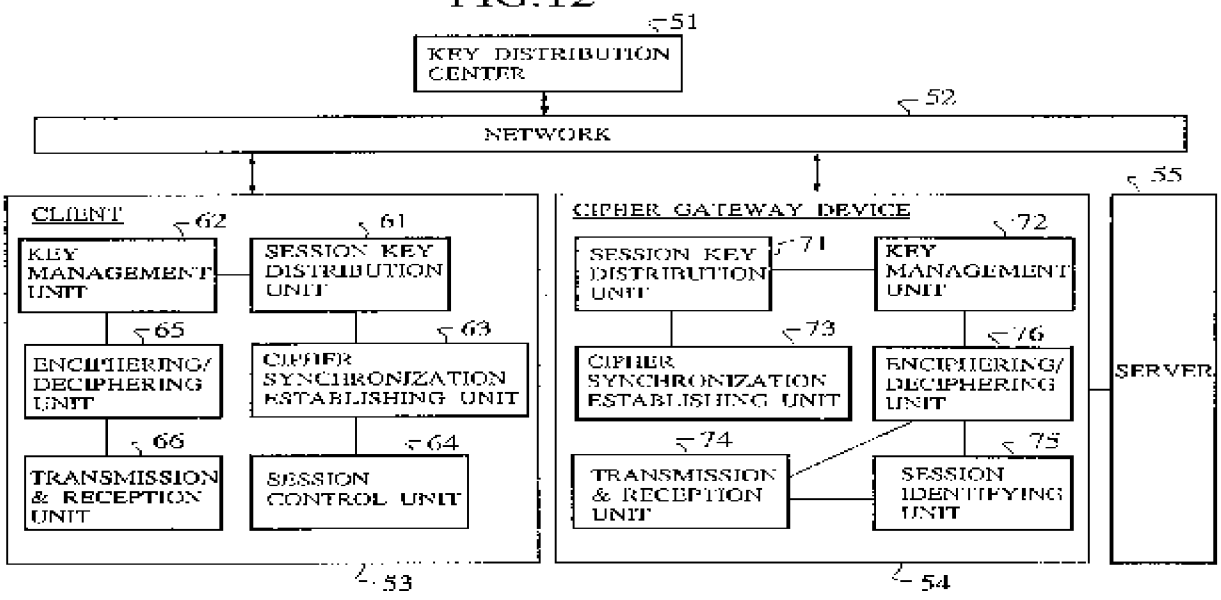
Therefore, it is respectfully submitted that the amendments raise no question of new matter and that claim 1, and claims dependent thereon are not definite.

35 U.S.C. § 102 Claim Rejections

Claims 1-6 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,604,807 (Yamaguchi et al.). Reconsideration is respectfully requested.

Yamaguchi et al. discloses a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware, and establishing a synchronization at the start and end of the cipher communication.[2] In particular, Yamaguchi et al. discloses, as shown in **FIG. 12** below, wherein each client **53** and each cipher gateway device **54** are connected with the key distribution center **51**, the network **52**, and the server **55**.[3] Further, Yamaguchi et al. discloses the cipher gateway

FIG. 12



[2] Yamaguchi et al. at ABSTRACT.
[3] *Id.* at **FIG. 12**; and column 10, lines 53-56.

device **54** or router receives the packet destined to the server **55** from the client **53**, and deciphers the packet by using the common session key Ks and that this deciphered packet (plain text packet) is transmitted to the server **55** to carry out the non-cipher communication between the cipher gateway device **54** and the server **55**.[4] Alternatively, Yamaguchi et al. discloses the cipher gateway device **54** or router receives the packet destined to the client **53** from the server **55** by the non-cipher communication, and enciphers the packet by using the common session key Ks and this enciphered packet is transmitted to the client **53** to carry out the cipher communication between the cipher gateway device **54** or router and the client **53**.[5]

However, Yamaguchi et al. nowhere discloses each and every limitation of amended claim 1, as required for an anticipation rejection. In particular, Yamaguchi et al. nowhere discloses:

> the apparatus including encryption/decryption means for performing an encrypting process and a decrypting process on data to terminate encryption-based security between the communications terminals having the encrypting capability and/or the non-encrypting capability; and
> . . . . *wherein the encryption apparatus further includes bridge means for allowing data to be outputted as it is from another port without any routing process; and*
>
> wherein the data has been received with one of the plurality of ports of the encryption apparatus and the encrypting or decrypting process has been performed on the data (emphasis added).

That is, Yamaguchi et al. nowhere discloses a configuration corresponding to the "bridge means" recited in claim 1. Moreover, Yamaguchi et al. nowhere discloses: "the encryption apparatus further includes *bridge means for allowing data to be outputted as it is from another port without any routing process*," as recited in amended claim 1.

Further, it is respectfully submitted that the conventional configuration of the background art, as disclosed by Yamaguchi et al. and shown in **FIG. 12** above, teaches away from the

[4] *Id.* at **FIG. 12**; and column 12, lines 50-56.
[5] *Id.* at **FIG. 12**; and column 12, lines 57-63.

claimed invention. In particular, a router of the background art, as typified by **FIG. 12 of** Yamaguchi et al. above, comprises encryption/decryption means *but does not include a bridge means*, as recited in the claimed invention. Further, it is requirement that the router itself have unique IP addresses that are different from the network addresses assigned to networks connected via the router. This requirement makes the initial and maintenance setup of addresses in the background art more complicated than that of the claimed invention.

Additionally, since a plurality of networks are connected via the router, different IP addresses need to be set for each port. As a result, IP addresses are different in the input and output of the router of the background art. When the router is inserted between terminals on the networks or detached from the terminals, not only do the addresses of the router itself need to be setup but also the addresses of terminals connected to the router need to be setup. This leads to much more cumbersome operating procedures for the background art routers, as typified by Yamaguchi et al., as compared to the claimed invention. This is further emphasized in the paragraph below.

In contrast to the background art, as typified by Yamaguchi et al., the use of the encryption apparatus comprising the "bridge means," as recited in amended claim 1: (1) requires *no IP addresses* of the encryption apparatus during data communications; (2) *allows IP addresses not to be changed* at an input port and output port of the encryption apparatus; and (3) *reduces troublesome operating procedures* such as those needed for setting addresses in system initialization and maintenance. Thus, the encryptions of the claimed invention are easily utilized in an office LAN or other applications. However, without the "bridge means," as recited in claim 1, Yamaguchi et al. cannot provide the advantages of the claimed invention discussed above and thus, Yamaguchi et al. teaches the approaches of the background art and *teaches away* from the claimed invention.

Conclusion

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00038-US1 from which the undersigned is authorized to draw.

Dated: September 12, 2007

Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Agent for Applicant